

# **INFORMATION OPERATIONS: A Look at Emerging Army Doctrine and its Operational Implications**

A Monograph  
By  
Major Kevin J. Doyle  
Military Intelligence

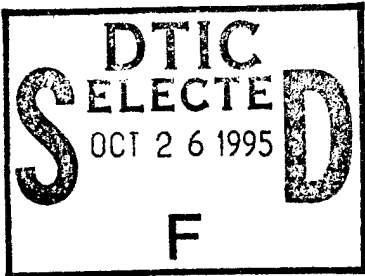


19951024 136

School of Advanced Military Studies  
United States Army Command and General Staff College  
Fort Leavenworth, Kansas

Second Term AY 94-95

Approved for Public Release; Distribution is Unlimited

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE		3. REPORT TYPE AND DATES COVERED
4. TITLE AND SUBTITLE INFORMATION OPERATIONS: A Look at Emerging Army Doctrine and its Operational Implications			5. FUNDING NUMBERS	
6. AUTHOR(S) Maj Kevin J. Doyle				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Command and General Staff College School of Advanced Military Studies Ft Leavenworth, KS, 66027			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES				
12a. DISTRIBUTION/AVAILABILITY STATEMENT Distribution Unlimited; Approved for Public Release			12b. DISTRIBUTION CODE	
13. ABSTRACT (Maximum 200 words)				
 <p style="text-align: right;">DTIC QUALITY INSPECTED 8</p>				
14. SUBJECT TERMS Information Operations, C2W, Command and Control Warfare, Information Warfare, FM 100-6, Information Age Warfare.			15. NUMBER OF PAGES 49 f3	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT U	18. SECURITY CLASSIFICATION OF THIS PAGE U	19. SECURITY CLASSIFICATION OF ABSTRACT U	20. LIMITATION OF ABSTRACT	

## GENERAL INSTRUCTIONS FOR COMPLETING SF 298

The Report Documentation Page (RDP) is used in announcing and cataloging reports. It is important that this information be consistent with the rest of the report, particularly the cover and title page. Instructions for filling in each block of the form follow. It is important to *stay within the lines* to meet *optical scanning requirements*.

**Block 1. Agency Use Only (Leave blank).**

**Block 2. Report Date.** Full publication date including day, month, and year, if available (e.g. 1 Jan 88). Must cite at least the year.

**Block 3. Type of Report and Dates Covered.** State whether report is interim, final, etc. If applicable, enter inclusive report dates (e.g. 10 Jun 87 - 30 Jun 88).

**Block 4. Title and Subtitle.** A title is taken from the part of the report that provides the most meaningful and complete information. When a report is prepared in more than one volume, repeat the primary title, add volume number, and include subtitle for the specific volume. On classified documents enter the title classification in parentheses.

**Block 5. Funding Numbers.** To include contract and grant numbers; may include program element number(s), project number(s), task number(s), and work unit number(s). Use the following labels:

<b>C</b> - Contract	<b>PR</b> - Project
<b>G</b> - Grant	<b>TA</b> - Task
<b>PE</b> - Program Element	<b>WU</b> - Work Unit Accession No.

**Block 6. Author(s).** Name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. If editor or compiler, this should follow the name(s).

**Block 7. Performing Organization Name(s) and Address(es).** Self-explanatory.

**Block 8. Performing Organization Report Number.** Enter the unique alphanumeric report number(s) assigned by the organization performing the report.

**Block 9. Sponsoring/Monitoring Agency Name(s) and Address(es).** Self-explanatory.

**Block 10. Sponsoring/Monitoring Agency Report Number.** (If known)

**Block 11. Supplementary Notes.** Enter information not included elsewhere such as: Prepared in cooperation with...; Trans. of...; To be published in.... When a report is revised, include a statement whether the new report supersedes or supplements the older report.

**Block 12a. Distribution/Availability Statement.** Denotes public availability or limitations. Cite any availability to the public. Enter additional limitations or special markings in all capitals (e.g. NOFORN, REL, ITAR).

**DOD** - See DoDD 5230.24, "Distribution Statements on Technical Documents."

**DOE** - See authorities.

**NASA** - See Handbook NHB 2200.2.

**NTIS** - Leave blank.

**Block 12b. Distribution Code.**

**DOD** - Leave blank.

**DOE** - Enter DOE distribution categories from the Standard Distribution for Unclassified Scientific and Technical Reports.

**NASA** - Leave blank.

**NTIS** - Leave blank.

**Block 13. Abstract.** Include a brief (*Maximum 200 words*) factual summary of the most significant information contained in the report.

**Block 14. Subject Terms.** Keywords or phrases identifying major subjects in the report.

**Block 15. Number of Pages.** Enter the total number of pages.

**Block 16. Price Code.** Enter appropriate price code (*NTIS only*).

**Blocks 17. - 19. Security Classifications.** Self-explanatory. Enter U.S. Security Classification in accordance with U.S. Security Regulations (i.e., UNCLASSIFIED). If form contains classified information, stamp classification on the top and bottom of the page.

**Block 20. Limitation of Abstract.** This block must be completed to assign a limitation to the abstract. Enter either UL (unlimited) or SAR (same as report). An entry in this block is necessary if the abstract is to be limited. If blank, the abstract is assumed to be unlimited.

### ABSTRACT

INFORMATION OPERATIONS: A Look at Emerging Army Doctrine and its Operational Implications by MAJ Kevin J. Doyle, USA, 49 pages.

This monograph discusses how the Information Revolution is leading the Revolution in Military Affairs. Specifically, it examines the operational implications of the changing information environment, the army's doctrinal response (Information Operations), and the utility of Information Operations.

The monograph examines the information environment and concludes that it gives nations and military forces unprecedented capabilities to acquire, manipulate, process and disseminate information. This implies that military forces will become much more efficient in maneuver, fires, and protection of forces. It also implies that information can be used as a separate element of combat power to attack directly the enemy's will to fight, to bolster US and coalition support for military operations, or to attack an enemy's information system to prevent him from doing the same. Because of this environment, information operations is emerging as a new area of warfare, and information is commonly considered as a fifth element of combat power.

The monograph then examines the army's doctrine for Information Operations (IO). It finds that the army primarily treats IO as a force multiplier which enables ground forces to maneuver, fire, and protect the force more efficiently, rather than implementing IO as an element of combat power. The army doctrine does not detail the capabilities of the present force structure to support IO, and suggests creating no new force or task organization. The doctrine recommends an assistant staff officer in the operations staff section to synchronize IO, without detailing the responsibilities inherent. The doctrine credibly treats IO as a supporting function which enables the force to develop the capability to execute simultaneous attack in depth. The monograph recommends additions or changes to the army doctrine as appropriate.

The monograph finally examines the implications of the environment, as well as the utility of IO, for the operational commander. It finds that the environment requires that the operational commander conduct information operations as part of every campaign, and that the commander should treat information operations as a separate combat function. It also recommends how the commander can use information operations to achieve the campaign end state.

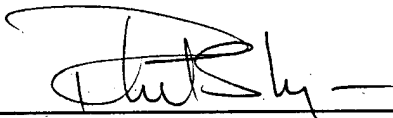
SCHOOL OF ADVANCED MILITARY STUDIES

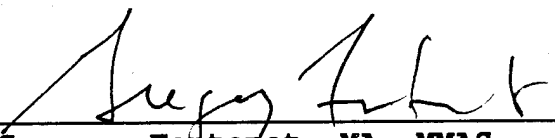
MONOGRAPH APPROVAL

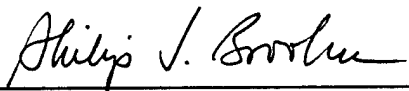
Major Kevin J. Doyle

Title of Monograph: Information Operations: A Look at  
Emerging Army Doctrine and its Operational  
Implications

Approved by:

  
\_\_\_\_\_  
LTC Robert L. Mayes Monograph Director

  
\_\_\_\_\_  
COL Gregory Fontenot, MA, MMAS Director, School of  
Advanced Military  
Studies

  
\_\_\_\_\_  
Philip J. Brookes, Ph.D. Director, Graduate  
Degree Program

Accepted this 19th Day of May 1995

Accession For	
NTIS CRA&I	<input checked="checked" type="checkbox"/>
DTIC TAB	<input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification	
By	
Distribution /	
Availability Codes	
Dist	Avail and/or Special
A-1	

## ABSTRACT

INFORMATION OPERATIONS: A Look at Emerging Army Doctrine and its Operational Implications by MAJ Kevin J. Doyle, USA, 49 pages.

This monograph discusses how the Information Revolution is leading the Revolution in Military Affairs. Specifically, it examines the operational implications of the changing information environment, the army's doctrinal response (Information Operations), and the utility of Information Operations.

The monograph examines the information environment and concludes that it gives nations and military forces unprecedented capabilities to acquire, manipulate, process and disseminate information. This implies that military forces will become much more efficient in maneuver, fires, and protection of forces. It also implies that information can be used as a separate element of combat power to attack directly the enemy's will to fight, to bolster US and coalition support for military operations, or to attack an enemy's information system to prevent him from doing the same. Because of this environment, information operations is emerging as a new area of warfare, and information is commonly considered as a fifth element of combat power.

The monograph then examines the army's doctrine for Information Operations (IO). It finds that the army primarily treats IO as a force multiplier which enables ground forces to maneuver, fire, and protect the force more efficiently, rather than implementing IO as an element of combat power. The army doctrine does not detail the capabilities of the present force structure to support IO, and suggests creating no new force or task organization. The doctrine recommends an assistant staff officer in the operations staff section to synchronize IO, without detailing the responsibilities inherent. The doctrine credibly treats IO as a supporting function which enables the force to develop the capability to execute simultaneous attack in depth. The monograph recommends additions or changes to the army doctrine as appropriate.

The monograph finally examines the implications of the environment, as well as the utility of IO, for the operational commander. It finds that the environment requires that the operational commander conduct information operations as part of every campaign, and that the commander should treat information operations as a separate combat function. It also recommends how the commander can use information operations to achieve the campaign end state.

Table of Contents	Page
I. Introduction.....	1
II. The Environment.....	4
III. Operational Implications of the Environment.....	6
IV. The Requirement for Information Operations.....	12
V. Emerging Army Doctrine: Information Operations.....	16
VI. Utility of Army Information Operations Doctrine.....	22
Recommendations.....	26
VII. Information Operations Considerations for Campaign Planning.....	30
VIII. Conclusion.....	40
Endnotes.....	42
Bibliography.....	45

## INTRODUCTION

Therefore I say: 'Know the enemy and know yourself; in a hundred battles you will never be in peril. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal. If ignorant of your enemy and of yourself, you are certain in every battle to be in peril.'<sup>1</sup>

Commanders have always recognized the value of accurate knowledge of METT-T to ultimate victory in war. Today, technology is driving a revolution in military affairs: the ability to acquire, control, and manipulate information not only will provide the conditions for successful maneuver, fires, and protection, but will also provide the commander a powerful, potentially decisive, new type of warfare. With the arrival of the "Information Age," the competition for information has become more technical and more important than ever before.

At the operational level, winning the fight for information gains the victor freedom of action. Military theorist Dr. James J. Schneider mentions the competition for freedom of action as an implication of the development of operational art:

Under the classical paradigm battles were waged to destroy the enemy's army. Under the new operational paradigm battles were fought to retain or deny freedom of action. Battles are seldom fought for the simple destruction of the enemy's forces....The idea of freedom of action implies that enemy destruction can be achieved better indirectly, that is, through envelopment and encirclement than through direct battle and attrition. Indeed, when freedom of action is lost, attrition ensues.<sup>2</sup>

With the introduction of railroads, the internal combustion engine, telegraph, wireless radio, tanks and combat aircraft, the search for operational freedom of action pointed military theorists toward maneuver and control of the air. Air superiority enabled ground units to move secure from air attack, and prevented the enemy from doing the same. Maneuver advocates such as Liddel Hart and Fuller championed a type of warfare intended to achieve victory by placing units in positions that paralyzed an enemy; the intent was to avoid "attrition war" by declining the slugfest. The result of successful maneuver would be that the enemy is placed in such a positional disadvantage that he chooses not to fight; choosing to fight despite the positional disadvantage, he would lose. The key to both maneuver and air superiority is that both ideas intend to preserve friendly freedom of action while denying the enemy's.

The technological developments of the Information Age offer a similar opportunity. The informational advantage gives the friendly commander the ability to see the enemy while preventing the enemy from seeing him, the ability to command and control his forces while denying the enemy the same capability, and the ability to use information to influence the enemy. An informational advantage allows air superiority, accurate targeting of indirect fire systems, effective maneuver, and the ability to directly attack the

enemy's will with information. Information dominance holds the promise of what maneuver warfare only hinted: presented with proof of his predicament, the enemy will either choose not to fight, or will fight at such a disadvantage (no freedom of action) that he will be destroyed very quickly.

Of course all of this assumes that US forces can in fact achieve information superiority. The army recognizes this is becoming a critical function. Training and Doctrine Command (TRADOC) is currently developing doctrine and concepts for Information Operations, which will be a new area of warfare intended to achieve and use this informational advantage as part of the joint team.

This monograph will examine the utility of Information Operations for the operational commander. It will examine the informational environment and analyze its implications for the operational commander, and then will analyze the emerging doctrine to discover how well it addresses the commander's needs. Finally, it will suggest how the operational commander can use Information Operations in his campaign plan to achieve his objectives.

## THE ENVIRONMENT

Information technology doubles roughly every one and a half to three years. Each successive generation is both faster but cheaper, smaller, and less power-hungry as well. Free silicon is inevitable; more precisely, unlimited amounts of information acquisition, processing, storage, and transmission capability will be available from indefinitely small and inexpensive packages. Limitations on information processing capability will constrain the conduct of neither military [nor] civilian operations.<sup>3</sup>

The removal of information processing constraints, married to the ongoing revolution in telecommunications and sensors, is causing what the Russians call a "Military Technical Revolution,"<sup>4</sup> or what is also referred to as a Revolution in Military Affairs. Modern military forces have the capability of collecting, analyzing, and disseminating huge quantities of information. This capability, combined with other technological improvements such as improved guidance and ballistics, global positioning systems, and improved sensors, give modern armies the theoretical capability to strike with all of their weapons simultaneously throughout the depth of the battlefield.

The civilian sector is making similar progress (in fact, it is leading the way in most areas). Information age technology is revolutionizing financial markets, manufacturing, civilian telecommunications, consumer goods, transportation - there is virtually no area that is not affected. Even in less developed areas of the world, advancements such as cellular phone technology are having a

significant effect. There is now a global internet that permits rapid sharing of data and databases between individuals and organizations across borders.

News media are quickly taking advantage of the revolution. Today virtually no significant action occurs anywhere in the world without international notice, except in those few areas of the world which have not been deeply penetrated by the media (North Korea comes to mind). Even that may soon change; national or international media will likely eventually own their own surveillance satellites or other covert surveillance means, and then be capable of broadcasting their own "intelligence updates" about events around the world.

## OPERATIONAL IMPLICATIONS OF THE ENVIRONMENT

The operational commander is primarily concerned with the sequencing of operations and campaigns to achieve strategic objectives.<sup>5</sup> The changes to the environment that are resulting from the information revolution will change the way operational commanders sequence operations, how they choose military conditions that achieve theater objectives, and how they design the theater of operations, in the following ways:

- All operational objectives have an informational component; this component is strengthened by easy access to information. This means that the success or failure of an operational mission will be judged not only by classical military definitions such as force destruction or seizing of terrain. Mission success or failure is subjective; success is in the eye of the beholder. Perhaps this has always been true; the difference now is that all military actions come under the immediate scrutiny of national and international press, as well as all interested parties (friendly, enemy, allied and neutral) with access to the press reports. The result is that the audience's (US public, Congress, coalition nations, etc.) perception of success or failure depends on what the expected result was prior to the event, whether the actions of the force met or exceeded the expected result (according to the press as well as the government and commander), and whether the cost was within

expected tolerance. *Perception Management* (a euphemism for propaganda) therefore becomes an important function for the operational commander as well as the NCA and the military strategic level of war.

Perception Management applies to both US and foreign audiences. Certainly operational commanders operate in a very restricted environment regarding the management of the perceptions of US audiences (for example, the army is restricted from giving false information to the press, or performing psychological operations on US citizens), but there is still a public affairs requirement to present information in the best manner to support the achievement of the operational objective. The perceptions of coalition allies, their supporting populations, and host nation populations are also important to the success or failure of the operational mission. As an example, the perception of mission success in an allied nation's popular press may be vitally important to the maintenance of a coalition. Or, the perception of US impartiality during a peacekeeping mission may be the key to the success of the mission.

- Military information systems may become an operational Center of Gravity. When Clausewitz wrote of the Schwerpunkt (Center of Gravity), he arguably was referring primarily to the concentration of the mass of the army<sup>6</sup>. Today, combat effects can be massed without the physical massing of units on the ground. Since information

technology enables the massing of fires without the massing of units, and holds the promise to allow the commander to maneuver forces that are greatly dispersed, a technologically advanced information system may actually constitute the Center of Gravity. The information system enables accurate positioning of forces, accurate, real time targeting, situational awareness, command and control, and a myriad other functions. As information technology brings new types of weapons such as lasers or directed energy weapons to the battlefield, an Information Age force will become even more dependent on its information system. The information system may become its "hub of all power and movement upon which everything depends."<sup>7</sup> Regardless, an enemy who can attack and defeat the information system of an information-based force (one heavily dependent on the ability to acquire, analyze, process and disseminate huge volumes of data very quickly, using advanced communications, computers, and sensors) will gain the freedom of action necessary to engage in a direct fire attrition fight (if that is his goal), or to destroy the enemy with his own information-based air power and maneuver (if his is also an information-based force).

- Establishing minimum information conditions will be a prerequisite to winning any future war. Information-based forces must establish the conditions necessary to exercise freedom of action in war or in operations other than war.

These information conditions will vary according to METT-T, but will generally be those conditions necessary to achieve the minimum required freedom of action that enables the force to achieve its mission. Some Russian theorists believe that we are entering an age that will require a military force to first win the information war, then the air war, then the ground war, with each phase setting the minimum essential conditions for the commencement of the next phase<sup>8</sup>. Operational commanders must establish the essential information conditions when sequencing operations and campaigns.

Winning the information war in an operation other than war is no less important. Information objectives will be described differently; it may be that maintenance of the proper perceptions will be the minimum necessary condition that allows the force the freedom to complete its mission.

- It will become possible to strike the enemy nearly simultaneously, with all of the weapons of the force, throughout the enemy's depth. The power of sensors, satellite communications and navigational aids, data processing, and precision guidance will allow simultaneous attack of the enemy throughout the depth of a theater of operations. Nuclear weapons and intercontinental ballistic missiles have made this a strategic capability for years; in the future operational commanders will achieve the same effect with far less collateral damage.

This will obviously affect the sequencing of operations and campaigns. It suggests the capability to fight an accelerated Desert Storm, with an initial operation designed to achieve information dominance, followed by a nearly simultaneous air and ground attack that destroys all enemy forces, perhaps in a matter of hours or days rather than weeks.

This development will put even more pressure on the operational commander to achieve information superiority early. Since information superiority will be a necessary precondition for any attempt at such a simultaneous attack, the force will be required to establish favorable information conditions to minimize the effects of an enemy strike and establish the conditions for the friendly strike.

- Protection of friendly information systems is critical. This implication is actually a direct result of the analysis suggesting that information systems may form an operational center of gravity. Even if these systems do not form the center of gravity, they will be indispensable to the concentration of the force's combat power, and therefore will demand protection similar to that usually accorded to the most critical and low density killing systems.

- The will of governments, non-state entities, and supporting populations is more accessible; it will be possible to attack directly an opponent's will with information. It is now easier to communicate directly with

an opposing leader, commander, or population. It is also easier to affect his information systems, both military and nonmilitary. Both possibilities offer the potential to attack directly an opponent's will with information. This has always been theoretically possible; the information revolution makes it easier, and our growing skill in information manipulation make the messages or effects potentially much more powerful than previously. For example, operational commanders will be able to use information to disrupt an opponent's financial structure, governmental control apparatus, or other key systems such as electrical power or communications. They will also be able to use information to change the perceptions of target populations or leaders. These capabilities can make information operations decisive, since they can attack directly the enemy's center of gravity or decisive points. Information operations will provide the operational commander a deterrent option which can end a campaign favorably without the use of lethal force.

## THE REQUIREMENT FOR INFORMATION OPERATIONS

The operational implications of the Information Age create a requirement for information operations. These operations should be designed to achieve those information objectives key to the operational commander.

The objectives of information operations for the operational commander can be stated as follows:

- Establish information control. This objective is similar to the Air Force objective to achieve air control. Just as it is difficult to conduct air operations against an enemy without first having achieved air superiority, it is difficult to conduct information operations in support of the force without first having achieved some degree of information control.

Information control should be measured by the *relative* freedom of action that the force enjoys when trying to execute functions, such as precision strike, air interdiction, ground maneuver, or subsequent information operations. One set of definitions for levels of information control, presented to the Army Roundtable on the Revolution in Military Affairs, follows:

**Information Supremacy** exists when a competitor can control all information on the battlefield. The enemy is helpless to acquire any relevant information or to discern the real from the imaginary. As a result, he cannot use information in an organized fashion to shape his operational plans. Nor, can the enemy deny information the competitor desires.

**Information Dominance** exists when a nation has

such an information advantage over his competitor that the enemy cannot employ information warfare in an effective fashion. Under Information Dominance, information control is not absolute. The nation without dominance may still be able to conceal some information from his enemy or to collect information from his competitor. Unlike Information Supremacy, the dominant nation will not be able to close off or shape all information sources at will. For instance, the US was unable to find Iraqi Scuds during the war, suggesting that the US had not achieved Information Supremacy, but did maintain Information Dominance because Saddam was compelled to seek less efficient means of Scud attack.

Information Superiority is a localized form of Information Dominance. It implies a sufficient information gap to allow a nation to perform a specific information warfare task at a specific time and place. A nation that has achieved Information Superiority will be able to carry out certain missions without interference from a competitor's information resources, but that superiority is not general and does not imply an ability to carry out all missions all the time. Unlike Information Dominance, a nation could have Information Superiority in one area and an inferiority in another.'

- Conduct information operations in support of other combat functions. Even while information control is being established, and throughout the rest of the war, operations are conducted to provide C2 of the force, to protect the force from enemy intelligence and killing systems, to ensure total asset visibility for logistic forces, to provide intelligence for targeting, situation assessment, etc., and to degrade enemy C2 in support of other operations. As forces become more technically proficient, this objective may be stated as conducting information operations to support simultaneous attack of the enemy throughout his

depth, while preventing the enemy from doing the same to friendly forces.

- **Achieve operational objectives.** As was stated in the previous chapter, every operational objective has an informational component. Perceptions of potential adversaries, allies, host populations, or the others may be important enough to warrant explicit statement as an objective in the campaign or operational plan. Additionally, information operations can be used to achieve the campaign end state.

A good example is the sporadic "hearts and minds" campaigns conducted during the Vietnam War. The conduct of a "hearts and minds" campaign implies that the campaign end state can be expressed in informational terms. The success or failure of the attempts to win over the South Vietnamese population, and to thereby prevent their support for the Viet Cong, is not the point. The point is that if a campaign objective can be measured in terms of a change in attitude or perception, as evidenced by specific actions, then the force is conducting an information operation to achieve the objective.

The information operations objectives stated above imply a total force effort. Information operations can be conducted primarily by units classically associated with the "infosphere", such as intelligence, signal, public affairs (PA), and psychological operations (PSYOP), or they may

expand to include Special Forces, precision strike weapons, Air Force units, and conventional maneuver forces. In all cases, the actions of the total force, subject to intense media scrutiny as they are, will have to be governed to avoid conflict with informational objectives.

This points to the requirement to plan and synchronize information operations as a separate function for the operational commander. Presently, the actions of intelligence, signal, PSYOP, PA, CA, EW, deception, and the rest of the force are synchronized strictly on an ad hoc basis. Planning and synchronizing these functions implies, at the least, a staff entity with coordinating authority, and possibly a subordinate unit task organized to conduct major portions of information operations.

This implies the operational commander should treat information operations as a combat function similar to maneuver or fires, rather than as a supporting function. There are certainly times when information operations will be conducted strictly as a supporting function, enabling the force to accomplish a mission related to force destruction, occupation of ground, or some other measure of success. However, there will be instances when the information operation is the first priority and the focus of the entire force. This argues for its treatment as a separate combat function to be synchronized with maneuver, fires, air defense, and other more traditional killing functions.

## EMERGING ARMY DOCTRINE: INFORMATION OPERATIONS

In Force XXI...America's Army of the 21st Century, the following objectives are stated for the future force: Dominate Maneuver, Conduct Precision Strike, Protect the Force, Project and Sustain Combat Power, and Win the Information War<sup>10</sup>. This highlights the importance that today's army leadership puts on achieving information superiority in any future conflict. The army is working to develop doctrine and organizations capable of winning the information war as part of the joint team.

The primary doctrinal publications dealing with information operations are TRADOC Pam 525-5, FORCE XXI OPERATIONS: A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early Twenty-First Century, Field Manual 100-6, Information Operations, and TRADOC Pam 525-XX, Concept for Information Operations. This chapter presents a review and evaluation of each.

TRADOC Pam 525-5 "describes the conceptual foundations for the conduct of future operations in War and OOTW involving Force XXI."<sup>11</sup> It provides guidance for the development of future doctrine and force structure, rather than doctrine for winning the information war today. Even so, it describes the army's vision of future operational environments, and introduces the concept of *Information Operations*<sup>12</sup> (IO), emphasizing the integration of IO into all operations, and the critical role of the commander in

directing IO<sup>13</sup>.

TRADOC Pam 525-5 mentions winning the information war as a "key component of depth and simultaneous attack"<sup>14</sup>:

These measures will include the establishment of electro-magnetic spectrum supremacy through nonnuclear electromagnetic pulse generators, space-based information denial systems, and computer viruses. Electronic warfare preparations will normally precede, but may take place concurrent with, ground and air operations. Command and control warfare (C2W) may replace air supremacy as the essential first step in operations. Television and other communications media provide means to defend or undermine the will of entire populations. Another method of attack will be to access the enemy battlefield computer systems and manipulate information. Through successful information operations, adversaries will be forced to exercise command through nineteenth century means, while US forces operate state-of-the-art, twenty-first century systems.

Although this description is specifically intended to describe how winning the information war supports depth and simultaneous attack, it actually describes information operations for a much wider spectrum of operations.

Finally, TRADOC Pam 525-5 introduces the idea that information may join maneuver, firepower, protection and leadership as a separate element of combat power<sup>15</sup>. FM 100-5 states that "Combat power is created by combining the elements of maneuver, firepower, protection, and leadership"<sup>16</sup>. The addition of information as a fifth element of combat power would imply that the achievement of information superiority or an information objective can be an end in itself, rather than a means to support the

operations of the force.

Field Manual 100-6, Information Operations, is the emerging doctrine which "integrates all aspects of information applicable to military operations."<sup>17</sup> It defines the components of Information Operations as command and control (C2) (both friendly and adversary), C2W, intelligence, and "that part of the GIE [global information environment] which influences military operations."<sup>18</sup> C2W includes the elements of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW), physical destruction, counterintelligence (CI), and information security (INFOSEC), supported by intelligence<sup>19</sup>. Finally, the GIE "is comprised of non-DOD information systems which collect, process, and disseminate information about operations."<sup>20</sup>

FM 100-6 sees Information Operations primarily as a force multiplier. It states that IO

is a force multiplier by allowing commanders to execute their decision cycle inside that of the adversary's. It supports the conduct of military operations...It enables and protects friendly information systems (FIS), synchronizes force application, connects hierarchical and non-hierarchical systems, establishes sensor-shooter-commander linkage, and denies adversary counter-C2 of friendly systems.<sup>21</sup>

Even in its chapter on IO support for operations other than war, FM 100-6 treats Information Operations as a supporting function, rather than an operation which may actually achieve a campaign objective. The sole exception is a

vignette on the last page of the manual which describes the importance of projecting the proper information in a peacekeeping operation<sup>22</sup>.

Another example of this approach is found under "Command and Control Planning Considerations" for IO. In this section FM 100-6 points out that commanders

must learn to identify and articulate their information needs. Commanders must also make known the value, priorities, and consequences associated with their information needs for their command. Each commander must strike a balance between too much and too little, recognizing that there will be errors of omission, commission, and costs associated with each. As a result the commander must convey his intent. It sets the objectives for IO, consequently enhancing his battle command capabilities.

Again, the emphasis is on what IO can do to support other operations of the command, rather than the potential objectives of the command which can be met by IO.

From an organizational perspective, FM 100-6 suggests the formation of an "IO cell charged with planning and coordinating IO."<sup>23</sup> This cell, similar to a targeting cell, would be formed according to METT-T and the IO requirements for specific operations. Additionally, the doctrine recognizes that a "virtual" IO cell (collocation not required) may be possible as better communications and processors become available. The document does not mention the possibility that the commander would consider task organizing a force to achieve IO objectives, or to synchronize the IO effort below the staff level.

The third army publication largely concerned with IO is TRADOC Pam 525-XX, Concept for Information Operations, a TRADOC publication which is intended to describe "how to win the information war in military operations now and into the 21st century."<sup>24</sup> It describes the objective of IO in similar fashion to FM 100-6 as "to enable, enhance, and protect the use of information in the friendly decision and execution process while influencing (degrading, controlling) an adversary's decisions and actions through manipulation of his information/ information system."<sup>25</sup> This again implies IO is a supporting system for the force. The document later implies that IO might be used to achieve strategic objectives of deterrence of hostilities, but that at the operational level the objective of IO is to restrict the adversary's battle space, while supporting the expansion of friendly battle space to the appropriate size for the mission.<sup>26</sup> Even so, the Concept does state that information is the fifth element of combat power, again implying more than simply a supporting role, even at the operational level<sup>27</sup>.

The Concept expands on the organizational approach taken by FM 100-6. While the field manual addresses the formation of an ad hoc IO Cell, the concept advocates the formation of a staff entity in the G-3 called the Commander's Information Operations Staff (CIOS) to be directed by the Commander's Information Operations Staff

Officer (CIOSO). However, the Concept falls short of advocating the creation of new positions to man the staff, instead stating that the representation will come from existing staff agencies as required.<sup>28</sup> The Concept, like the field manual, is mute on the question of task organization for IO.

## UTILITY OF ARMY INFORMATION OPERATIONS DOCTRINE

In order to judge the utility of emerging army Information Operations doctrine for the operational commander, it is necessary to judge how well the doctrine addresses the operational requirement. A doctrine for Information Operations should recognize the operational implications of the environment, and should address how IO can be used to achieve informational objectives. Finally, it should address how the army intends to synchronize operations, and what units or means will be used in Information Operations. It is important to note that neither of the doctrinal publications dealing specifically with Information Operations are final, so some changes to the doctrine may occur. This analysis examines the draft doctrinal manuals.

Emerging army IO doctrine does not recognize all of the operational implications of the environment. The doctrine credibly treats those areas in which IO is addressed as a supporting function for existing military functions. It is weak in its treatment of IO as a function which may achieve operational objectives as a primary, rather than supporting function.

It states that it is now theoretically possible to attack the enemy simultaneously throughout his depth, and that IO is key to this capability<sup>29</sup>. The requirement to collect, analyze, and disseminate information from sensor to

shooter very quickly is clearly understood and described.

It recognizes the criticality of the Friendly Information System, and the obvious requirement to protect it. It does not state that force information systems may become operational centers of gravity or decision points for attack; this perhaps is implied by the very creation of the IO function. However, it may also reflect a bias to treating IO as a supporting function for other operational functions.

The doctrine does not adequately address all of the possible objectives for IO. The FM 100-6 and TRADOC Pam 525-XX statements about the purposes of IO focus on IO support to battle command, IO support to simultaneous attack, IO support to split based operations and to force logistics. The stated purposes do not exclude the use of IO to achieve operational objectives; in fact, the Concept mentions the objective of "influencing (degrading, controlling) an adversary's decisions and actions through manipulation of his information/ information system."<sup>30</sup> The problem lies primarily in emphasis. Both the Field Manual and the Concept view IO as primarily a function which can allow the army to do better and faster what it already does, which is to maneuver and kill the enemy with fires.

Although the emerging doctrine recognizes that IO may be used to achieve an objective, such as managing perceptions in a peacekeeping operation, and influencing the

population's perception of the government during post-conflict activities<sup>31</sup>, it does not state that IO will have a role in the achievement of the informational component of all operational objectives.

The other area in which IO has a lead role is in the establishment of information conditions required before the initiation of other operations. Although our doctrine recognizes this possibility, it does not dwell on it, apparently because the US generally assumes that it will not have to fight to achieve information superiority prior to a future conflict. Again, the doctrine does not exclude this type of operation, and the possibility is inherent in the purpose of IO.

The concept that information is the fifth element of combat power is a powerful one. Maneuver, firepower, protection, and leadership have traditionally comprised the elements of combat power; information has always been implied in the command and control aspect of leadership. The addition of information implies that superior information is combat power. It also implies that superior information can be used not only to support the other four elements, but to have its own influence on the battle. Finally, it implies that the other elements of combat power could be used to support the application of information. These implications, while not stated in the doctrine, support the development of total force Information

Operations.

Emerging IO doctrine does not "break any rice bowls" in its organizational approach. Given the stated criticality of information operations in future conflict, the establishment of no more than an information operations staff officer is an evolutionary, minimalist approach. Both FM 100-6 and the Concept establish the idea of an Information Operations staff cell as part of the G-3, similar to a targeting cell or a deep operations cell. In both of the documents, the cell is taken out of current resources.

The army doctrine thus far has not developed the responsibilities of the IO staff. The Concept states that the Commander's Information Operations Staff will organize, plan, and execute IO, and that the staff requires representation from the G-2, G-6, and the areas of C2W, EW, OPSEC, PSYOP, military deception, and fire support (and others as necessary)<sup>32</sup>. The doctrine does not specify the products of the staff, and perhaps goes too far to say that the staff will "execute" IO.

The army IO doctrine lists those functions which are part of Information Operations, but does not deal with units or task organization which might be required to meet information objectives. FM 100-6 mentions the formation of an IO cell as the primary organizational implication of the new doctrine, but does not discuss required units below the

staff level. The Concept for Information Operations simply states that "Implementation of revised doctrine can impact on the overall force design and/or organizational designs."<sup>33</sup>

### Recommendations

The army has a good start toward developing a doctrine for Information Operations. It should not be surprising that the doctrine is incomplete or inconsistent in some areas, given the newness of the concepts and the difficulty in changing an army in the midst of a technical revolution. The army and the Department of Defense have to balance the arguments of the true revolutionaries such as Martin Libicki, who advocate the creation of a separate Information Corps within DoD<sup>34</sup>, and those who believe that information is still simply a commodity which supports other functions, similar to fuel or food. Nonetheless, the following recommendations are offered which can strengthen army Information Operations doctrine:

Accept the premise that information is the fifth element of combat power. The army has stated that information is or will become the fifth element of combat power<sup>35</sup>. As it begins to accept and internalize this idea, its implications will become clearer. Information control, the achievement of informational objectives, and the provision of information support to the force will become combat functions. Concepts of operation will address

maneuver, fires, and information rather than just maneuver and fires. Operational information will be managed as an operational level operating system along with movement and maneuver, fires, protection, command and control, intelligence, and support. In short, a new area of warfare will be created, with all that implies for doctrine, organization, training, leader development, manning and sustaining the force.

Develop information operations doctrine to achieve campaign objectives as well as to support other operations. The informational component of all operational objectives, combined with the availability and public access to operational information, implies that the force must conduct an information operation as part of every operation. The army should develop information operations to achieve appropriate information conditions for the commander, to achieve campaign information objectives, and to provide information support to other combat functions. The army will then be able to offer Information Operations as a deterrent option which can be tailored to achieve a campaign objective of deterrence, or as a warfighting function which can achieve the informational component of the campaign end state.

Doctrine should highlight the concept of information control as a pre-condition to other operations; this would help operational planners sequence operations and design

deployment plans accordingly.

Develop specific staff functions for Information Operations. The IO staff officer, whether he is a coordinating staff officer or an assistant, will require a dedicated staff. The size, composition, and training of the staff will be based on the responsibilities of the cell.

In order to size the staff, the army needs to define the required products from the IO staff, based on the objectives of IO. This should be developed and included in the new Field Manual, so that current army commanders will be able to plan and execute Information Operations in support of the operational commander. An operational level IO staff must be capable of:

- Performing mission analysis to determine IO missions specified and implied, as well as facts and assumptions impacting on IO.
- Determining the informational component of the operational objectives and end state.
- Developing objectives for IO which support the achievement of the operational end state.
- Determining the forces required, and developing a plan to achieve the IO objectives.
- Recommending priority intelligence requirements for support of IO.
- Determining measures of effectiveness which can be used to determine the effectiveness of IO. These measures

will drive additional intelligence requirements (for IO BDA).

Describe present information operations capabilities of army forces, and define considerations for organization for combat. Since FM 100-6 is intended to be used as doctrine for units in the field, rather than as a concept for future force development, it should include a more detailed look at the type units and capabilities available to the commander for IO. It also should address the issue of establishing Information Operations Task Forces in order to better plan, synchronize and execute IO below the staff level.

The doctrine defines IO as including C2, C2W (OPSEC, military deception, PSYOP, EW, CI, INFOSEC, and physical destruction), intelligence support, and "that part of the GIE which influences military operations"<sup>36</sup>. These functions can not be combined in one unit; FM 100-6 implies this when it states: "The C2W part of IO is not a system. It is a strategy that synchronizes and integrates various assets and techniques of the five primary C2W components..."<sup>37</sup>. What should be done is to break out IO by the type of objective or operation to be conducted, and then to consider the issue of units and task organization accordingly. The result would be a section which explains the capabilities and limitations of army units conducting IO today, and how to integrate their efforts, depending on the type of information operation being conducted. This would

aid the operational commander employing army IO capabilities for the joint IO effort.

#### INFORMATION OPERATIONS CONSIDERATIONS FOR CAMPAIGN PLANNING

The information revolution has established an environment which requires operational commanders to conduct information operations, whether they call them by that name or some other. Commanders will be required to deploy forces and conduct operations to establish favorable information conditions in which to operate; they will conduct operations to collect, process, analyze, and disseminate information in support of all of their other operational functions; and they will conduct operations to ensure that the informational components of their campaign objectives are met. These requirements have probably existed since armies developed command structures, and certainly since the development of independent press reporting of combat operations. The capabilities and proliferation of modern information systems have simply placed greater emphasis on an already important area of warfare.

Following is a brief outline of the information operations considerations which operational commanders should integrate into their campaign planning. It is based on the fundamentals of operational planning and on the concepts of theater and operational design from FM 100-5, Operations, and on the emerging army doctrine for Information Operations. It addresses the requirements of an

operational commander preparing a campaign plan using today's forces and the emerging doctrine.

### Fundamentals of Operational Planning

**Mission.** Mission analysis results in facts, assumptions, specified and implied tasks, essential tasks, and finally, a restated mission for the command as a whole. Unless the national command authority or the joint force commander specify some informational mission in their order, informational tasks will be developed as implied tasks. In order to develop the necessary implied tasks, the commander must identify the minimum essential information control (supremacy, dominance, superiority) which will set the necessary conditions for the achievement of the campaign objectives; determine the information requirements which must be met to support other missions; and determine what the informational end state must be for him to achieve mission success (required perceptions, etc.).

In peacetime, the US military has a mission of deterrence<sup>38</sup>. Operational commanders develop Flexible Deterrent Options to give the national command authority options short of war which may achieve campaign objectives, and to buy time in case deterrence fails. Information operations may become the FDO of choice for operational commanders. FDOs are "intended to facilitate early decision by laying out a wide range of interrelated response paths that begin with deterrent-oriented options carefully

tailored to *send the right signal*"<sup>39</sup> (italics added).

"Sending the right signal" implies an information operation; an operation which combines conventional military activities, PSYOPS, proper use of the press, and neutralization or manipulation of enemy information systems will provide the operational commander a powerful FDO which will be capable of ending a campaign without the use of lethal force. Since information operations are designed to control information and influence enemy perceptions, as well as to manipulate or degrade enemy information systems, they can be used to convince an enemy not to go to war.

The mission analysis should also consider the capabilities and limitations of all units which might contribute to information operations. Since there are no "informational units" per se, this analysis must be performed by the information operations staff and the commander.

**Commander's Intent.** Normally, the commander's intent will address the purpose, method and end state for the campaign or operation. The commander will define the extent of his information operation by defining the purpose and end state for the overall campaign or operation. If the end state can be measured in terms of informational control, or measured in informational terms, such as the perceptions of an enemy or an audience, then the command may actually be conducting an information campaign, rather than using

information operations to support other operations.

An information campaign differs from an information operation only in the importance of informational objectives to the campaign end state. If the end state can be measured primarily in informational terms such as enemy perceptions or the manipulation of enemy information systems, rather than traditional terms such as force destruction or occupation of ground, then the focus of the entire command will be on the information operation, and the actions of the command will be prioritized accordingly.

A campaign's character is determined primarily by its end state. If the campaign end state includes the destruction or neutralization of enemy air forces, then an "air campaign" may be required. Similarly, if the end state includes the destruction of ground forces or the occupation of ground, then a "ground campaign" will be conducted. Finally, if the information operation is a primary effort of the operational commander, based on his analysis of the required end state, then he can be said to be conducting an information campaign.

**Estimates.** Estimates for the information operation will require a change in emphasis of the normal estimate process, not a change in the process. From the perspective of the intelligence estimate, operational forces will need very detailed intelligence on enemy military and civilian information systems and processes, and on enemy reliance on

those systems. Enemy population and leader perceptions, and enemy vulnerabilities to friendly information operations will also be key pieces of information. Informational environmental analysis will also be required. This will include perceptions of other than US audiences important to the campaign, such as coalition populations and host nation populations or leaders, as well as information such as host nation electromagnetic spectrum control, and weather impacts on information operations.

There is a requirement for extensive peacetime analysis and preparation of the battlefield. If it is accepted that the initial establishment of information superiority is likely to be key to future victory, then it will be critical to be prepared to fight the information war as early as possible to reduce our vulnerability to an early enemy strike. It will be necessary to maintain standing, detailed data bases for contingency areas in support of early information operations.

From the friendly perspective, the information operations staff must be expert in analyzing unit capabilities to determine what they add to the Friendly Information System, as well as what they can contribute to the information war. The staff must be able to determine the forces required to fight the information operation, and recommend the proper deployment sequence for these forces. This analytical requirement would be mitigated by an army

doctrine which establishes guidelines for the use of army units in information operations.

**Concept of Operations.** FM 100-5 states that the concept of operations must address, at a minimum, the scheme of maneuver and the concept of fires.<sup>40</sup> If it is true that information is becoming the fifth element of combat power, or if the informational end state is critical to the command's mission, then the operational commander should address, as a minimum, his concept for maneuver, fires, and information operations.

Given the state of emerging army doctrine, this may be the hardest part of the information operation to develop. As has been shown, the capabilities and limitations of army units for information operations, as well as guidance for task organization and other related issues, are not addressed in the doctrine. Information operations staffs will be required to develop objectives, tasks and purposes for multiple units to achieve an informational end state. This will require knowledge about how to measure success, and how to determine whether enough force is available to accomplish the necessary tasks. A process for measuring informational correlation of forces has not yet been developed, so much of this analysis will likely be intuitive. Until the army develops a branch or specialty charged with training information operators, the commander should send his army information operations staff officers

to the Joint Command and Control Warfare Staff Officer's Course for training in an important part of information operations.

Will. FM 100-5 states that "Ultimately, the focus of all combat operations must be the enemy's will."<sup>41</sup> FM 100-6 supports this concept:

Because leaders are the main source of will in a military organization, our strategic and operational plans should employ IO to analyze the source of the adversary's will through every means available. Commanders may prepare concepts for IO that combine C2W means with messages delivered by PA and PSYOP forces that change the attitude or behavior of key audiences necessary to sustain his will.<sup>42</sup>

The traditional manner of attacking an opponent's will involved destroying or threatening to destroy his force, undermining the support of his power base, diplomatic pressure, or some other relatively indirect means. These measures will still be important, and perhaps primary, but are greatly strengthened by the addition of synchronized information operations. Information operations will ensure that the proper message of deterrence is actually received by a potential enemy, may threaten direct action through information means (such as computer viruses used to attack an enemy's financial structure), and can degrade an enemy's C2 system to such a point that the clearest message he receives from the theater of war is controlled and manipulated by US forces. For the first time, a means exists with the potential to attack directly an opponent's

will.

### Concepts of Theater and Operational Design

Center of Gravity. A case has been made that the information system may be a center of gravity for an Information Age force. If this is true, then those who believe that winning the information war may be all that is required for victory in the next war may be correct. COL Warden has written that the strategic leadership of a nation, or, at the operational level, the military commander of the forces in the theater of war, is a center of gravity. He also believes that the enemy's ability to command is usually the most important of the potential centers of gravity, but is also one of the most difficult to attack.<sup>43</sup> General (R) Glenn K. Otis has also written "The combatant that wins the information campaign prevails. We demonstrated this lesson to the world: information is the key to modern warfare -- strategically, operationally, tactically, and technically."<sup>44</sup> FM 100-5 also acknowledges that an enemy's national will or his C2 structure may constitute a center of gravity.<sup>45</sup>

As usual, good analysis is the key. Just as it was possible to lose in Viet Nam with overwhelming air superiority, it will be possible to lose the next war despite information superiority. If our analysis shows, however, that the enemy center of gravity is his information system, then our ability to conduct information operations

to attack his system will be the key to the entire campaign. Conversely, if our center of gravity is our information system, then the component parts of that system must be protected as our first priority.

**Lines of Operation.** Lines of operation "define the directional orientation of the force in time and space in relation to the enemy."<sup>46</sup> FM 100-6 states that "IO provides an expanded capability to concentrate a multitude of forces and capabilities whose effects converge on the enemy by observing, recognizing the opportunity, and acting before he can effectively respond."<sup>47</sup> This implies that information operations tend to make the force more able to operate on multiple or exterior lines of operation while still being able to concentrate combat power. Lines of operation will remain important as long as it is necessary to move mass from the base to the objective; IO allows the force to decrease its vulnerability to enemy attack of single lines by providing the capability to attack with and sustain dispersed forces, and the theoretical capability to attack an enemy simultaneously throughout his depth.

**Decisive Points.** Decisive points are the keys to attacking the center of gravity.<sup>48</sup> If the enemy information system is a center of gravity, it is likely to be well protected, hidden, diffuse, redundant, and secure. In short, it will be extremely hard to attack. The key to winning the information operation to take down his center of

gravity will be the determination of the decisive points which allow attack of his information system. This analysis will be critical, and must be a focus of the informational preparation of the battlefield. The operational commander faced with a very sophisticated information system must ensure that he has available the skilled analysts required to break down this system (even if this means he must contract for them).

**Culmination.** Successful information operations will provide the commander enhanced awareness of his own and his enemy's situation, better enabling him to avoid culmination. Conversely, it can be used to convince an enemy that he has culminated, or hide the fact of his culmination from him if that is the goal of the operation. Since culmination is relative, the commander that wins the information war will be better able to determine and avoid his culminating point, and bring the enemy to his.

In planning, the operational commander's staff must also consider the culminating point of the information operation. Since information operations can use virtually all capabilities of the force, in many ways the culminating point may be similar to that for a conventional maneuver operation. For other types of information operations, however, the culminating point may be more a measure of human endurance and analytical capability under the stress of ever increasing information flow, than a measure of

information equipment differential.

#### CONCLUSION

The environment of war and other military operations is rapidly changing due to the Information Revolution. As operational commanders seek freedom of action, operations which provide the commander the ability to command and control his forces and see the enemy, while denying the enemy the same capability will become critical. Additionally, the ability to use information to achieve the operational end state increases.

The information environment now requires commanders to achieve information control to win; it also requires commanders to synchronize the operations of his information systems and the global information environment. Information operations is the army's answer to this requirement.

The army's emerging doctrine rightly identifies the need to synchronize information operations, and identifies an information operations staff to do this. However, while it provides a purpose for information operations at a conceptual level, it does not provide a method for planning and executing information operations using today's units, and does not speculate on the type units which may be required to execute the doctrine in the future. It also does not adequately deal with the possibility that information operations may be the force primary effort in some future operations.

Even though the doctrine is not yet completely developed, operational commanders can still use the concept of information operations in their campaign planning. The commander must identify the information conditions required to fight the rest of his campaign, and must identify any informational end states which must be achieved. He must perform a thorough informational preparation of the battlefield (or have access to it) early in order to help ensure favorable early conditions for the information fight. He must sequence his operations properly, perhaps fighting an information "campaign" in order to win subsequent operations or campaigns. He must protect his information system as the potential center of gravity which it is. Finally, he must be flexible enough to adapt to a campaign in which the information operation, using information as the fifth element of combat power, is the main effort of the entire force.

## ENDNOTES

1. Sun Tzu, The Art of War, translated by Samuel B. Griffith (New York: Oxford University Press, 1980), 84.
2. Schneider, James J., Vulcan's Anvil: The American Civil War and the Emergence of Operational Art, (Ft Leavenworth, KS: CGSC School of Advanced Military Studies, 16 June 1991), 34.
3. Libicki, Martin C., The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon (Washington, DC: National Defense University Institute for National Strategic Studies, March 1994), 7.
4. Mary C. Fitzgerald, "Russian Views on Information Warfare", Army (Arlington, VA: Association of the US Army, VOL 44, No. 5, May 1994), 57.
5. US Army, Field Manual 100-5, Operations (Washington, DC: Department of the Army, 14 June 1993), 1-3.
6. Schneider, James J., The Theory of Operational Art (Ft Leavenworth, KS: US Army Command and General Staff College, 1 March 1988), 26-27.
7. US Army, FM 100-5, Operations, 6-7.
8. Fitzgerald, 57.
9. Laurence Zuriff, "Understanding Information War" (a working paper), from The US Army Roundtable on the Revolution in Military Affairs (McLean, VA: Science Applications International Corporation, September 1993), 2.
10. US Army, Force XXI...America's Army of the 21st Century (Washington, DC: Department of the Army, 15 January 1995), 6-7.
11. US Army TRADOC Pam 525-5, FORCE XXI OPERATIONS: A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early Twenty-First Century (Ft Monroe, VA: HQ TRADOC, 1 August 1994), iii.
12. Ibid., 3-9.
13. Ibid., 3-7.
14. Ibid., 3-11
15. Ibid., 3-9.

16. US Army, FM 100-5, Operations, 2-9.
17. US Army, Field Manual 100-6, Information Operations (Coordinating Draft) (Ft Monroe, VA: HQ TRADOC, 22 July 1994), viii.
18. Ibid., viii-ix.
19. Ibid., ix.
20. Ibid., 1-5.
21. Ibid., 1-1.
22. Ibid., 7-8.
23. Ibid., 4-7.
24. US Army, TRADOC Pam 525-XX, Concept for Information Operations (Final Draft) (Fort Monroe, VA: HQ TRADOC, 5 May 1994), 3.
25. Ibid., 3-1.
26. Ibid., 3-4.
27. Ibid., 4-2.
28. Ibid., 4-5.
29. US Army, TRADOC Pam 525-5, FORCE XXI OPERATIONS: A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early Twenty-First Century, 3-9.
30. US Army, TRADOC Pam 525-XX, Concept for Information Operations (Final Draft), 3-1.
31. US Army, FM 100-6, Information Operations (Coordinating Draft), 7-8 and 4-2.
32. US Army, TRADOC Pam 525-XX, Concept for Information Operations (Final Draft), 4-4 to 4-5.
33. Ibid., 4-6.
34. Libicki, 50-69.
35. US Army, TRADOC Pam 525-5, FORCE XXI OPERATIONS: A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early Twenty-First Century, p. 3-9, and TRADOC Pam 525-XX, Concept for Information Operations (Final Draft), 4-2.

36. US Army, FM 100-6, Information Operations (Coordinating Draft), ix.
37. Ibid., 1-4.
38. The White House, A National Security Strategy of Engagement and Enlargement, (Washington, DC: US Government Printing Office, July 1994), 6-7.
39. National Defense University Armed Forces Staff College, AFSC Pub 1: The Joint Staff Officer's Guide (Washington, DC: National Defense University, 1993), I-15.
40. US Army, FM 100-5, Operations, 6-6.
41. Ibid., 6-7.
42. US Army, FM 100-6, Information Operations (Coordinating Draft), 4-5.
43. John A. Warden III, COL, "The Enemy as a System", Airpower Journal (Maxwell AFB: Airpower Research Institute, AL, Vol. IX, No. 1, Spring 1995), 49.
44. Glenn K. Otis, GEN (R), Concept Paper: Information Campaigns, (Ann Arbor, MI: Vector Research, Inc., 1991), 1-1.
45. US Army, FM 100-5, Operations, 6-7.
46. Ibid., 6-7.
47. US Army, FM 100-6, Information Operations (Coordinating Draft), 4-6.
48. US Army, FM 100-5, Operations, 6-8.

## BIBLIOGRAPHY

### Books

- Bellamy, Chris. Future of Land Warfare. New York: St Martin's Press, 1987.
- Brown, LTG (Ret) Frederick J. The US Army in Transition II. Washington, DC: Brassey's Inc, 1993.
- Campden, Alan D., ed. The First Information War. Fairfax, VA: AFCEA International Press, 1992.
- Collins, John M. Military Space Forces: The Next 50 Years. Washington, DC: Pergamon-Brassey's 1989.
- Friedman, Richard S. Advanced Technology Warfare: A Detailed Study of the Latest Weapons and Techniques for Warfare Today and Into the 21st Century. New York: Harmony Books, 1985.
- Libicki, Martin C. The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon. Washington, DC: National Defense University, March 1994.
- Littlebury, F. E. Invisible Combat: C3CM: A Guide for the Tactical Commander. Washington, DC: AFCEA International Press, 1986.
- McKnight, Clarence E. Control of Joint Forces: A New Perspective. Fairfax, VA: AFCEA International Press, 1989.
- Munro, Neil. The Quick and the Dead: Electronic Combat in Modern Warfare. New York: St Martin's Press, 1991.
- Orr, George E. Combat Operations C3I: Fundamentals and Interactions. Maxwell AFB: AL, Air University Press, 1983.
- Rice, Edward E. Wars of the Third Kind. Berkeley, CA: University of California Press, 1988.
- Rice, M. A. Communications and Information Systems for Battlefield Command and Control. London/Washington: Brassey's, 1989.
- Rosen, Steven. Winning the Next War. Ithaca, NY: Cornell University Press, 1991.
- Schwartau, Winn. Information Warfare: Chaos on the Electronic Superhighway. New York: Thunder's North Press, 1994.
- Taylor, Philip M. War and the Media. New York: Manchester University Press, 1992.

Toffler, Alvin and Heidi. War and Anti-War. Boston/New York: Little, Brown, and Company, 1993.

Warden, John A. III. The Air Campaign. Washington, DC: National Defense University Press, 1988.

#### Manuals

US Army Training and Doctrine Command. TRADOC Pamphlet 525-5, Force XXI Operations. FT Monroe, VA: Department of the Army, HQ, US Army TRADOC, 1 August 1994.

US Army. FM 100-5, Operations. Washington, DC: Department of the Army, June 1993.

US Army. FM 101-5, Command and Control for Commanders and Staff (Final Draft). Washington, DC: Department of the Army, 1994.

US Army. FM 100-6, Information Operations (Draft). Washington, DC: Department of the Army, 1994.

Joint Chiefs of Staff. Joint Pub 3-0, Doctrine for Unified and Joint Operations. Washington, DC: Joint Chiefs of Staff, September 1993.

Joint Chiefs of Staff. Joint Pub 3-13, Command and Control Warfare (2nd Draft). Washington, DC: Joint Chiefs of Staff, September 1994.

Joint Chiefs of Staff. Joint Pub 5-0, Doctrine for Planning Joint Operations. Washington, DC: Joint Chiefs of Staff, 1994.

Joint Chiefs of Staff. C4I for the Warrior. Washington, DC: Joint Chiefs of Staff, 12 June 1992.

US Army. Draft Army Concept for Command and Control Warfare. Ft Leavenworth, KS: US Army CAC, 1994.

#### Periodicals

"Army Plan Fosters Dynamic Information War Framework." Signal (48 no. 3), November 1993.

"Commanders Pull Intelligence Information Warfare Strategy." Signal (48 no. 12), August 1994.

"Constrained War." Parameters (Vol XXIII, No 2), Summer 1992.

"Future Operations." Military Review (Vol LXXIII), November 1993.

- "Information Dominance Edges Toward New Conflict Frontier."  
Signal (48 no. 12), August 1994.
- "The Nature of Future War." Jane's Intelligence Review (Vol 4, No 12), 1 December 1992.
- "Planning for a Future War." Jane's Intelligence Review (Vol 4, No 8), 1 August 1992.
- Beedham, Brian. "Defense in the 21st Century." The Economist, 5 September 1992.
- Bodnar, John W., CAPT (USN). "Military Technical Revolution: From Hardware to Information." Naval War College Review (46 no. 3), Summer 1993.
- Bodner, Seth. "Defense Planning in the New Global Security Environment." Army (43 no. 8), August 1993.
- Fitzgerald, Mary C. "Russian Views on Information Warfare." Army (44 no. 5), May 1994.
- Franke, MAJ Henry G. III. "Hyperwar: Brief, Violent, and Decisive." Army Times, 7 June 1993.
- Johnson, Craig L. "Information Warfare -- Not a Paper War." Journal of Electronic Defense (17 no. 8), August 1994.
- Libicki, Martin C., and Hazlett, James P. "Do We Need an Information Corps?" Joint Force Quarterly (no. 2), Autumn 1993.
- Ross, Jimmy D. GEN. "Winning the Information War." Army (44 no. 2), February 1994.
- Ryan, Donald E. "Implications of Information-Based Warfare." JFQ (No. 6), Autumn-Winter 94/95.
- Strain, Frederick R. "The New Joint Warfare." JFQ, Autumn 1993.
- Warden, John A. III, COL. "The Enemy as a System." Airpower Journal (Vol. IX, No. 1), Spring 1995.

#### Research Papers and Reports

- Barker, Richard, et al. Future Window of the Battlefield.  
Seattle, WA: Boeing Aerospace Company, January 1990.
- Bernard, Jacqueline M. Electronic Warfare Support: Training for Future Threats? Monterey, CA: Naval Postgraduate School, July 1991.

Biddle, Stephen D., and Victor A. Utgoff. The Battlefield for the Future. Alexandria, VA: Institute for Defense Analysis, January 1989.

Bigney, Russell E. et al. Exploration of the Nature of Future Warfare. Carlisle Barracks, PA: The Army War College, June 1974.

Blank, Stephen J. Afghanistan and Beyond: Reflections on the Future of Warfare. Carlisle Barracks, PA: The Army War College Strategic Studies Institute, 1993.

Bouton, D. A. US Military and Future War: Ready or Not. Carlisle Barracks, PA: The Army War College, May 1987.

Department of Defense. Conduct of the Persian Gulf Conflict: An Interim Report to Congress. Washington, DC: July 1991.

Dubik, LTC James M., and GEN Gordon R. Sullivan. Land Warfare in the 21st Century. Carlisle Barracks, PA: US Army War College Strategic Studies Institute, February 1993.

The Future Battlefield. The NATO Defense Research Group 25th Anniversary Seminar Proceedings, Vol 2, October 1992.

Future Vision: A Capabilities-Based Army for Transition into the 21st Century. Leavenworth, KS: The Titan Corporation Battle Command and Training Division.

Greer, MAJ James K. Operational Art in a Multi-Medium Environment. Ft Leavenworth KS: Command and General Staff College School of Advanced Military Studies, 29 June 1990.

"Integrated Space Systems Shape Future Battlefield". Signal (Vol 45, No 10), June 1991.

Joint Chiefs of Staff. Memorandum of Policy No. 30 Command and Control Warfare. Washington, DC: Joint Chiefs of Staff, 8 March 1993.

Jordan, Thomas M. MAJ. The Operational Commander's Role in Planning and Executing a Successful Campaign. Ft Leavenworth, KS: Command and General Staff College School of Advanced Military Studies 91-92.

Otis, Glenn GEN, and Cherry, W. Peter. Concept Paper: Information Campaigns. Ann Arbor, MI: Coleman Research Corporation and Vector Research, Incorporated, 19 November 1993.

Rinerson, Harley D. Communications and Imaging Technology: Revolutionizing Command and Control of the Future Battlefield. Ft Leavenworth, KS: US Army Command And General Staff College, 7 June 1991.

Schneider, James J. The Theory of Operational Art (Theoretical Paper No. 3). Ft Leavenworth, KS: US Army Command and General Staff College School of Advanced Military Studies, 1 March 1988.

Schneider, James J. Vulcan's Anvil: The American Civil War and the Emergence of Operational Art (Theoretical Paper No. 4). Ft Leavenworth, KS: US Army Command and General Staff College School of Advanced Military Studies, 16 June 1991.

Strategic Studies Institute. . Campaign Planning. Carlisle Barracks, PA: US Army War College, 4 January 1988.

Strategic Assessment Center. The US Army Roundtable on the Revolution in Military Affairs. Falls Church, VA: Science Applications International Corporation, September 1993.

US Army. TRADOC Pam 11-9, Blueprint of the Battlefield. Ft Monroe, VA: US Army TRADOC, 10 May 1991.

Vector Research, Inc. Concept of the Information Campaign -- Initial Insights into its Development and Execution -- (Volume I: Final Briefing). Ann Arbor, MI: Vector Research, Inc., 22 July 1993.